@DeldigiKNOW

December 2017 Issue

DEPARTMENT OF TECHNOLOGY & INFORMATION

DELIVERING TECHNOLOGY THAT INNOVATES

# *e*Security Newsletter — New Device?

Getting a new device is EXCITING! But take a few minutes to consider the best way to secure your new device against the non-stop security threats against you, your device and your data.

## A NEW DEVICE WON'T SECURE ITSELF!

INSIDE YOUR CONNECTED HOME:

*Protect Your Always-On Family*

Every day, your house connects to the internet in ways you might not even realize – today's appliances, toys, lighting, TVs, cameras are rapidly advancing in technology. And outside your home, there's so much more that's connected – from your car to the roads you travel on to your whole city.

**Protect all Internet of Things (IoT) devices.** Protecting devices like wearables and smart appliances can be different than securing your computer or smartphone. Do the research before you make a purchase and take steps to secure the device over time.

**For each device you have, use strong, unique passphrases, pattern, or biometric authentication.** Use a screen-lock option when available. For all new devices change the default password.

**Update Operating Systems and Applications when the update becomes available**. Doing so ensures you have the latest protection against known vulnerabilities.

**Lock down your Login.** Strengthen accounts by using the strongest authentication available such as biometrics, security keys or a unique one-time code through an app on your mobile device. Usernames and passwords often are not enough to protect email and banking accounts.

**Set privacy restrictions.** No matter which cloud option you use (Dropbox, OneDrive, iCloud, Google Drive, etc.), set restrictions on your files and only share them with those you intend. Use two-factor authentication for all of your accounts.

**Use anti-malware.** Some software includes features that allow you to set up automatic backups and find your device should it be misplaced or stolen.

**Disable Bluetooth and location tracking**. Don't turn them on until you need them. Avoid using these features in public areas.

**Review your phone apps regularly.** Delete the ones you don't use and be selective when installing new apps. Use trusted sources and avoid apps that require unnecessary access to personal information. Don't freely give apps device permissions they don't need (camera, microphone) and consider not allowing apps to run in the background.

**Treat your devices like you would your cash.** Maintain control of mobile devices in public areas and if you travel consider using a locking security device and tracking and recovery software.

### Be a Part of Something Big

Get involved and promote a safer, more secure Internet.
Visit https://staysafeonline.org/

*Questions, comments or topic suggestions?*
Email us at eSecurity@state.de.us.

Visit the DTI eSecurity website for previous issues

*e*Security Newsletters

DigiKnow
CYBER SECURITY DEPENDS ON YOU

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to http://extranet.dti.state.de.us/information/dtie_information_eSecurity.shtml (link only works if you view this while connected to the state network).